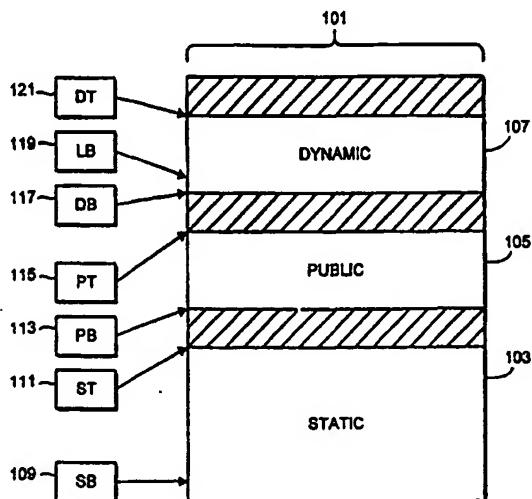




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10</b>		<b>A2</b>	(11) International Publication Number: <b>WO 98/52159</b>
			(43) International Publication Date: 19 November 1998 (19.11.98)
(21) International Application Number: PCT/GB98/01390 (22) International Filing Date: 14 May 1998 (14.05.98) (30) Priority Data: 60/046,514      15 May 1997 (15.05.97)      US 60/046,543      15 May 1997 (15.05.97)      US 09/064,915      23 April 1998 (23.04.98)      US (71) Applicant: MONDEX INTERNATIONAL LIMITED [GB/GB]; 47-53 Cannon Street, London EC4M 5SQ (GB). (72) Inventors: EVERETT, David, Barrington; 31 Ashdown Avenue, Saltdean, Brighton, East Sussex BN2 8AH (GB). MILLER, Stuart, James; 9 Woodford Green, The Warren, Bracknell, Berks RG12 9YQ (GB). PEACHAM, Anthony, David; 4 Lynwood, Groombridge, Tunbridge Wells, Kent TN3 9LX (GB). SIMMONS, Ian, Stephens; The Elms, School Road, Broughton, Cambs PE17 3AT (GB). RICHARDS, Timothy, Philip; 32 Craig Mount, Radlett, Herts WD7 7LW (GB). VINER, John, Charles; Hydes, Woodlands Lane, Windlesham (GB). (74) Agent: POTTER, Julian, Mark; D. Young & Co., 21 New Fetter Lane, London EC4A 1DA (GB).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).  Published <i>Without international search report and to be republished upon receipt of that report.</i>	

(54) Title: MULTI-APPLICATION IC CARD WITH DELEGATION FEATURE



## (57) Abstract

A multi-application IC card which processes two or more applications using an Application Abstract Machine architecture. The AAM architecture only allows one application to be executed at a time and allows for shared processing by performing a delegation function to a second application. A data space for each application is allocated when the application is selected to be executed. The data space includes a volatile and non-volatile region. The delegation function temporarily interrupts the execution of the first application, saves the temporary data of the first application, shares any data needed with the second application and the second application is executed until the delegated task is completed. The first application then retrieves the saved data and completes its execution. A delegator stack is used to keep track of the delegator's identity when multiple delegations occur. The AAM model allows for a high level of security while transferring data between applications.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

MULTI-APPLICATION IC CARD WITH DELEGATION FEATURE

### BACKGROUND OF INVENTION

5 Integrated circuit ("IC") cards are becoming increasingly used for many different purposes in the world today. An IC card (also called a smart card) typically is the size of a conventional credit card which contains a computer chip including a microprocessor, read-only-memory (ROM), electrically erasable programmable read-only-memory (EEPROM), a random access memory (RAM), an Input/Output (I/O)  
10 mechanism and other circuitry to support the microprocessor in its operations. An IC card may contain a single application or may contain multiple independent applications in its memory. MULTOS™ is a multiple application operating system which runs on IC cards, among other platforms, and allows multiple applications to be executed on the card itself. The multiple application operating system present on the IC card allows a card  
15 user to run many programs stored in the card (for example, credit/debit, electronic money/purse and/or loyalty applications) irrespective of the type of terminal (i.e., ATM, telephone and/or POS) in which the card is inserted for use.

A conventional single application IC card, such as a telephone card or an electronic cash card, is loaded with a single application card and only executes that one  
20 application when inserted into a terminal. For example, a telephone card could only be used to charge a telephone call and could not be used as a credit/debit card. If a card user desires a variety of application functions to be performed by single application IC cards issued to him or her, such as both an electronic purse and a credit/debit function, the card

user would be required to carry multiple physical cards on his or her person, which would be quite cumbersome and inconvenient. If an application developer or card user desired two different applications to interact or exchange data with each other, such as a purse application interacting with a frequent flyer loyalty application, the card user would be  
5 forced to swap multiple cards in and out of the card-receiving terminal during the transaction, making the transaction difficult, lengthy and inconvenient.

Therefore, it is beneficial to store multiple applications on the same IC card. For example, a card user may have both a purse application and a credit/debit application on the same card so that the user could select which type of payment (by  
10 electronic cash or credit card) to use to make a purchase. Multiple applications could be provided to an IC card if sufficient memory exists and an operating system capable of supporting multiple applications is present on the card.

The increased flexibility and power of storing multiple applications on a single card create new technical challenges to be overcome concerning the integrity and  
15 security of the information (including application code and associated data) exchanged between the individual card and the application provider as well as within the entire system when communicating information between applications.

For instance, the existence of multiple applications on the same card allows for the exchange of data between two applications, while one of the applications  
20 is being executed. As stated above, a frequent flyer loyalty program may need to be accessed during the execution of an electronic purse application. If data is passed

between applications in an insecure manner, it may be possible for a third party monitoring the transaction to determine the contents of the transferred data or even other private data associated with one or both of the applications. Thus, it would be beneficial to provide an application architecture and memory organization which protects an  
5 application's data from being discovered by a third party when it is exchanged with other applications present on the IC card.

Accordingly, it is an object of embodiments in accordance with the invention to provide an application architecture and memory organization which provides for data interaction between applications having increased security and allows multiple  
10 applications to be accessed while performing a desired task or function.

### SUMMARY OF THE INVENTION

15 The present invention provides for a multiple application architecture for an IC card called an application abstract machine (AAM) and a method for implementing that architecture. The processing of multiple applications is accomplished by generating for at least one application (the "first application") a data memory space including at least two segments, a volatile memory segment and a non-volatile memory segment,  
20 commencing the execution of the first application's instructions; delegating or switching execution from the first application to the delegated application and in so doing, saving any data generated by the first application in the logical data memory space associated with the first application; executing the second application's instructions; retrieving the

saved data and completing with this data the execution of the first application's instructions.

Additional delegation commands can be issued by the second application or other subsequent applications. The command delegated is interpreted by a delegated application in the same manner as a selection command being issued directly by a terminal and therefore each application performs the security functions at the same level as if a terminal is issuing the command.

The volatile memory segment can further be separated into public ("Public") and dynamic ("Dynamic") portions. Data can be exchanged between a plurality of applications and/or a terminal when stored in the Public region of the data memory. The Dynamic memory region can be used solely as temporary work space for the specific application being executed.

#### BRIEF DESCRIPTION OF THE DRAWINGS

15

Further objects, features and advantages of embodiments of the invention will become apparent from the following detailed description taken by way of example only and in conjunction with the accompanying figures showing illustrative embodiments of the invention, in which

20

Fig. 1 is block diagram illustrating the data memory space segment and associated registers for an IC card application using the AAM organization;

Fig. 2 is a block diagram illustrating the code memory and the data memory spaces for an IC card application using the AAM architecture;

Fig. 3 is a flow diagram illustrating the steps of performing a request for a delegation function by one application to another;

5 Fig. 4 is a flow diagram illustrating the steps of performing a return delegation control function for a delegate application to a delegator application;

Fig. 5 is a flow diagram illustrating the steps of performing an inquire delegator ID request of a delegation function;

10 Fig. 6 is a block diagram of an IC card chip which can be used as a platform in accordance with the invention; and

Figures 7A, 7B and 7C illustrate multiple delegation calls made between three applications.

Throughout the figures, the same reference numerals and characters, unless otherwise stated, are used to denote like features, elements, components or  
15 portions of the illustrated embodiments. Moreover, while the subject invention will now be described in detail with reference to the figures, it is done so in connection with the illustrative embodiments. It is intended that changes and modifications can be made to the described embodiments without departing from the true scope and spirit of the subject invention as defined by the appended claims.

20



DETAILED DESCRIPTION OF THE INVENTION

An embodiment of the present invention provides for a method and  
5 apparatus for processing multiple application programs with associated data stored on an  
IC card which can be accessed and executed. An application stored on the card can be  
selected by a terminal, or other interface device, or another application. Each application  
program which is stored on the IC card when executed is allocated a memory space  
organized by the program's software code (instructions which are executed by a  
10 processor located on the IC card) and the associated data which the application stores and  
uses during execution of the program.

For example, a multi-application card may store a purse application, or an  
electronic money application, and a specific loyalty application such as a frequent flyer  
awards application. Each application has software code and associated data to support  
15 the execution of that software code. Each application is allocated a memory space when  
executed. In this example, there is interaction between the two applications stored on the  
card. For each dollar electronically spent to make a purchase, the user may be entitled to  
one frequent flyer mile which is stored and processed by the frequent flyer program. The  
purse application need not be aware of the specific loyalty program stored on the card,  
20 but instead may contain an instruction to communicate with any loyalty program stored  
on the card. The loyalty program will require input data representative of the amount of  
a particular electronic value so that it can update its own stored data of current frequent  
flyer miles for the user of the card.

When two applications need to communicate during the same transaction, a system architecture is required to process both applications in an efficient and secure manner. One approach could be a windows type model where both applications could be running at the same time. Presently, however, IC card platforms are not powerful enough  
5 to simultaneously operate multiple programs efficiently. Also, transferred data may be exposed to unwanted third party access. To address this problem, embodiments in accordance with the current invention, which is described in greater detail below, selectively interrupt the execution of applications in a secure manner. This allows the integrity of the applications' data to be maintained and allows the best utilization of the  
10 available memory space in the IC card.

An efficient architecture for processing multi applications in an IC card is termed an Application Abstract Machine (AAM) architecture and is described herein. The AAM Architecture applies to any platform independent of its hardware and enables developers to write applications to store on the IC cards which are portable across many  
15 different types of platforms (e.g., IC cards built by different manufacturers with different processor configurations) without the need for knowledge about the specific hardware of the platform.

An application abstract machine (AAM), a term for the memory allocation and organization for the data stored and used by each application, is created for each  
20 application stored on the IC card which is executed by the processor on the card. In order to ensure data integrity and security when data is transferred between applications which

are executed on the IC card, only one application on the IC card is allowed to be executed at a time. Each application has a data memory space which is virtually allocated and mapped onto the physical memory addresses available in the IC card memories. Data is then passed between two or more applications within a specified memory location and in a manner consistent with transferring data to an external terminal or device with which the IC card is securely interacting. At a general level, each AAM space created for each application being executed includes two separate address spaces, one for the program code itself and one for the program data which is stored and/or used by the application. The program data address space is effectively divided into three segments: a Static segment, a Dynamic segment and a Public segment which are described in more detail in conjunction with Figure 1. As stated above, the Static, Dynamic and Public segments are logically mapped to the physical memory; they are virtual memory segments as opposed to physical memory segments. The AAM data address space is preferably addressed and processed using seven different address registers and two control registers.

Figure 1 shows an illustrative diagram of a logical data space allocation 101 created for an application used in conjunction with the present invention. The AAM data portion 101 includes a Static data space 103, a Public data space 105 and a Dynamic data space 107. Also shown are a series of address registers: the Static base address register 109, the Static top address register 111, the Public base address register 113, the Public top address register 115, the Dynamic base address register 117, the Dynamic top address register 121 and local base address register 119 which serves as a local stack

frame pointer in the Dynamic data space when the application is being executed. The address registers can contain physical memory addresses but preferably contain offset addresses for the various data address spaces in order to be hardware independent. An example of the overall address space is 64K bytes, although the size varies with the applicable platform and the available memory size. The registers can also be considered pointers or can be any other conventional addressing mechanism.

Within the allocated AAM data space 101, the Static portion of the memory is non-volatile which is not erased after power is removed from the IC card (such as EEPROM), the Dynamic space is volatile (such as RAM) which may be erased after power is removed from the card and the Public space is also volatile (such as RAM). An IC card can receive power from a terminal after it is interfaced into the terminal. Although an IC card may contain a battery to maintain some power for memory and circuitry, volatile memory will typically be erased after the IC card is removed from its power source.

The defined AAM data space has bytes in each segment which are contiguous, so that applications can perform pointer and offset arithmetic. For example, if the segment addresses "1515" and "1516," or any other pair of sequential numbers, are both valid and are present within the same segment, then they address adjacent bytes. This allows offset values stored in registers to determine the location of a desired memory address. The segment address of the first byte of the Static segment is zero, so that the segment address of a given location within the Static region is equal to its offset.

Pointers to other specific regions of the Static data area can be stored in the Static data because the Static region is non-volatile. For example, if the card user's name is stored in the Static memory of a credit/debit application, the application will know the card user's name will always be stored in the 5<sup>th</sup> memory location above the starting point for the Static portion of memory. The location can be noted as SB[5] or the 5<sup>th</sup> byte above the Static Bottom. Since the Static memory is non-volatile, it will not be erased after each transaction and the application will always know of its location relative to the Static segments' address registers.

On the other hand, the segment address of any location in the Dynamic or Public segments is not always equal to a particular offset from the beginning of the respective segment because the contents of those segments change for each operation. The fourth location in the Dynamic segment will be different for each operation performed by the application. The address of a memory location of Dynamic or Public segment is fixed preferably only for the duration of one command-response pair operation. Because segment addresses in Dynamic or Public are not fixed, MULTOS Executable Language (MEL)<sup>TM</sup> instructions (or any other program instructions) cannot refer to data using only segment addresses. Instead, a tagged address preferably is used to identify data which is to be retrieved, manipulated, transferred and/or stored with the IC card system.

A tagged address is a nineteen bit value consisting of a three bit tag (address register number) and a sixteen bit offset. Each of the seven address registers for

the AAM data space contain a segment physical address. For instance, the address registers SB 109 and ST 111 point to the boundaries of the Static, the address registers PB 113 and PT 115 point to the boundaries of the Public and the address registers DB 117 and DT 121 point to the boundaries of the Dynamic. For each segment, the top register points to the byte immediately after the last valid byte. For example, the last valid byte of the Static is ST[-1]. Register LB functions as a stack frame pointer. It points to a location in the Dynamic segment to indicate a specific byte of local data for the currently executing application.

Referring to Figure 1, the allocated Static segment 103 contains the application's non-volatile data. Static data includes data which is associated with each application for every transaction such as the card user's name, account number, PIN value and address. Static data also includes variable data which is stored for use in future transactions using the application. For example, in a purse transaction, the electronic value data would be read from the Static segment and later saved in the Static segment at the end of the transaction. Additionally, transaction information data or available credit limits in the case of a credit/debit application would be stored in Static data.

The Static data is addressed using register SB (Static Base) and the register ST (Static Top) as offset registers. These registers contain the offset value from a physical address in a memory on the IC card. The individual memory location is then further offset from these starting points such as SB[3] or ST[-5]. SB is defined as zero and ST is equal to the size of the application's Static data which is set when the

application is loaded onto the IC card. The multiple application operating system ensures that no other application can read or write the data stored in the Static segment of a particular application. Using current technology, the Static segment is preferably mapped onto an EEPROM (Electrically Erasable Programmable Read-Only Memory) which is  
5 non-volatile.

The Dynamic segment 107 contains the application's volatile or temporary data. Dynamic data includes data which is temporarily used during the execution of an application such as intermediate values used in calculations or working variables. For example, a purse application may temporarily store the value of a transaction in order to  
10 reduce the amount of the value in the purse. The temporary data is used much like conventional computer programs use RAM to perform their assigned operations. The Dynamic segment preferably is divided into two parts, the session data portion and the stack data portion. The size of the session data is a constant for each application and is determined when the application is loaded. The stack holds variable data which is unique  
15 to the particular transaction being executed. The stack data portion stores data in a last-in-first-out manner. The stack is initially empty, but expands and contracts during execution of the application.

The Dynamic data is addressed from the register DB 117 to register DT 121. Register LB 119 serves as a local stack frame pointer to particular memory  
20 locations in the Dynamic segment for delegate commands or function calls. Register LB 119 is used to address the topmost frame, that of the currently executing function's

session data. Register DT 121 serves as an address offset for the stack pointer. A one byte data item at the top of the stack is addressed as DT[-1], the next byte below is addressed by DT[-2], and so on. A push operation increments the relative value of DT for each item on the stack and a pop operation decrements the relative value of DT for each item on the stack. For example, a data element located at DT[-5] will be located at DT[-6] after an additional data item is placed on the stack.

When an application is being executed, the Dynamic segment created for that application also contains the application's session data which is used in performing the assigned task(s) or operation(s). The multiple application operating system ensures that no other application can read or write the data stored in the Dynamic segment of a particular application. The session data is set to zero upon the start of the execution of the application. Stack data will be saved in the stack if the application delegates a task or operation to another application.

A delegation function occurs when one application selects another application to process a command instead of processing the command itself. An example of a delegation function occurs when a delegator application receives a command that it does not recognize or is not programmed to process. The selected application should not reject the command and provide an error response to the interface device (IFD), but instead should pass the command to the appropriate receiver, or delegated application. In order to perform a delegation, the delegator calls the Delegate primitive. The Delegate primitive is a subroutine recognized by the multiple application operating system which



is executed when the operating system interprets the Delegate instruction. Primitives can be stored as part of the operating system itself, loaded as a separate routine when the operating system is installed. Primitives are preferably written in machine executable language so that they can be executed quickly although they could be written in a higher level language. When a Delegate command is executed, execution of the delegating application is suspended, and the delegated application is executed instead. The delegated application then generates its own data memory space according to the AAM architecture. The data stored in the Public memory space of the first application (stored in RAM) is sent to the Public memory space of the second application (which could be physically the same memory but is allocated separately for each application) so that data can be passed between the applications. The Dynamic memory space is also shared although data is saved in a stack for the delegator and the other portions initialized before the delegated application is executed because the Dynamic data is secret.

In most cases, the delegated application processes the command exactly as though the command has arrived directly from an interface device. When the delegated application has finished processing the command, and has written a response into the allocated Public memory segment, it exits as normal. The delegator then resumes execution at the instruction address following the executed instruction which called the Delegate primitive. The response generated by the delegated application is retrieved or accessed from the allocated Public memory space. The delegator application may simply

exit in turn, thus sending the response to the IFD, or may carry out further processing before exiting.

Another example of a delegation operation occurs when two applications need to share data. If an application A always returns a data item N when processing a command B, then another application which also returns data item N in response to a command can delegate the function B to application A in order to reduce the need for duplicate codes stored on the IC card. For example, if a PIN needs to be checked before an application is executed, an application stored on the card can delegate the "retrieve PIN function" to a PIN application which returns a stored universal PIN for the card.

10 Preferably, a new session begins whenever the IFD, e.g. a terminal, successfully selects an application, even if the application has been previously selected during the transaction. For example, if a card user goes to a terminal and transfers twenty dollars of electronic cash using a purse application, charges thirty dollars using a credit/debit application and then transfers ten dollars using the purse application again, 15 three separate sessions will have occurred even though only two applications were used during the entire transaction. Each time an application delegates a task or function to another application, the delegated application treats the delegate function as if the IFD devices had selected the application to perform the task or function. However, performing a delegation function as described below has a different effect on session 20 data.

The following examples will help explain when the session data is initialized (i.e., erased) versus when it is saved to be used in further operations. If application A is selected by an IFD device, and receives commands X, Y and Z from the terminal, application A may delegate all three commands to application B. For example, 5 delegations may occur in response to delegation commands in the program code. Both applications A and B will have their session and stack data in their respective Dynamic segments initialized (set to zero) when they receive command X, but the stack will not be initialized when they receive the subsequent commands Y and Z.

In a second example, application A is selected, and receives commands X, 10 Y and Z from the terminal. Application A processes X itself, but delegates Y and Z to application B. Application A will have its session and stack data initialized when it receives X, but not when it receives the subsequent commands Y and Z. Application B will have its session and stack data initialized when it receives Y, but not Z.

One example of a use of session data is to support the use of a session 15 Personal Identification Number (PIN). The application could reserve one byte of session data to support the PIN-receiving flag. On receiving the PIN check command, the selected delegated application could update the flag as follows: if the PIN command is received and the inputted PIN is equal to the stored pin, then it will set the session data DB[0] to 1. If not, the application will check if the PIN flag is already set by checking 20 the value in DB[0]. In either of the above cases, the application will process the rest of the commands in the session because the PIN has been verified. If neither of the cases is

true, then the application will not process the command because the PIN is not proper.

The PIN checking function could be a delegated function from the selected application to a PIN checking application.

The Public segment 105 is used for command and response data being  
5 passed between an IFD and an application. During a delegate command, the Public segment contains the data passed between two applications, the delegator (the application initiating the delegation) and the delegated application (the application which performs the delegated function). An application may also use the Public segment as a further temporary working storage space if required. The Public data is addressed using offsets  
10 stored in register PB 113 as a starting address, to register PT 115 as an ending address. Register PB 113 and Register PT 115 are fixed for the duration of a command-response pair being initiated by the IFD or delegator. Public data can include data inputted into or supplied by a terminal such as a transaction amount, vendor identification data, terminal information, transmission format or other data required or used by an application resident  
15 on the IC card. Public data can also include data which is to be transmitted to an IFD device or other application such as an electronic dollar value, card user information transmission format or other data required or used by the terminal or other delegated application.

The multiple application operating system ensures that the data stored in  
20 the Public segment remains private to the application until the application exits or delegates. Preferably, the data in the Public segment is then made available to other

entities as follows: (1) if the application delegates, the whole of the Public segment becomes available to the delegated application; (2) if the application exits, and is itself delegated by another, the whole of the Public segment becomes available to the delegator; or (3) if the application exits, and is not itself delegated, then a portion of the Public  
5 segment containing the I/O response parameters and data are made available to the IFD.

An application may write secret data into the Public memory segment during execution of the application, but the application must make sure it overwrites the secret portion of the Public segment before delegating or exiting. If the application abnormally ends (abends), then the operating system on the IC card preferably overwrites  
10 all of the data in the Public segment automatically so that no unwanted entities can have access to the secret data. If the MULTOS carrier device (MCD) is reset, the operating system overwrites data in the Public segment automatically, so that no secret data is revealed. A portion of the Public memory segment is also used as a communications buffer. The I/O protocol data and parameters are preferably stored at the top of the Public  
15 memory space. In another preferred embodiment, the top seventeen bytes are reserved for the communications protocol between the IFD device and the IC card application. However, additional or less bytes can also be used depending upon the particular application and operating system being utilized.

The spaces shown between the memory segments in Figure 1 will vary  
20 depending upon the specific application and commands being processed. There could be

no memory space between the memory segments so that the memory segments are contiguous.

Figure 2 shows an extended illustration of the AAM implemented architecture. Data memory space 201 includes the three segments Static, Public and  
5 Dynamic as previously described. Code memory space 203 contains the program instructions for an application stored on the IC card. The application instructions are preferably stored in an executable form which can be interpreted by the resident operating system but can also be stored in machine executable form. Instruction 205 is stored at one location in the code memory space 203. Additional instructions are stored in other  
10 locations of memory space 203. Two additional registers 207 and 209 are used in the AAM architecture. A code pointer (CP) register 207 indicates the particular code instruction to be next executed. In the figure, the register indicates, e.g., through an offset or pointer means, that instruction 205 is the next to be executed. Condition Control Register 209 contains eight bits, four of which are for use by the individual application  
15 and four of which are set or cleared depending upon the results of the execution of an instruction. These condition codes can be used by conditional instructions such as Branch, Call or Jump. The condition codes can include a carry bit, an overflow bit, a negative bit and a zero bit.

All address and control registers are set to defined values prior to  
20 executing the selected or delegated application. The values are set either when the application is first loaded onto the card and the size of the code and non-volatile data can

be ascertained or at the moment when the application passes control to the application.

When the application is loaded, SB is set to zero and ST is equal to the number of bytes in the application's Static database. The other address registers are initialized when the application is given control. CP 207 is set to zero and all eight bits in CCR 209 are  
5 cleared at the start of executing the application.

A communications interface mechanism is present between the IFD and an application which includes the use of the Public data segment as a communications buffer for command-response parameters. A command-response parameter means an application is given a command to perform and returns a response to the entity issuing the  
10 command. Applications interact with an IFD by receiving commands, processing them and returning responses across the IFD-Application Interface. When an application has completed executing a command, the application will place the response into the Public segment starting at PB[0] which can be read by the IFD device and will set the proper interface parameters in the reserved Public space relative to PT[0].

15 While an application can be called directly from an IFD and return a response directly to an IFD, it can also delegate a request to another application where appropriate. The subsequently-called application will then process the request on behalf of the first application. The delegation can be directly in response to a received command in which the delegator acts as a controller for delegating commands or subcommands to  
20 other appropriate applications. Alternatively, the delegated command can be embedded in an application's code which delegates control of the processor when the first

application needs to interact with another application during its execution, such as updating frequent flyer miles or verifying a PIN.

Figure 3 shows a flow chart of the steps which are performed when a delegate request is executed. Step 301 sets the parameter named `delegator_application_id` (delegator ID) to be equal to the `selected_file.application_id` (selected ID). The selected ID indicates the current application which is selected and which is currently being executed. The delegator ID indicates the application which delegates a function to another delegated application stored on the IC card. Step 303 then pushes (stores) the delegator ID onto the top of the `delegate_id_stack` (delegate stack). The data referenced in the Dynamic portion of allocated memory is saved so that the current application can complete its execution after the delegated function is complete. Data which is to be shared with the delegated application is referenced in the Public portion of allocated memory. The delegate stack is preferably stored outside of an application's AAM memory space and keeps track of which applications have delegated functions. Each application is suspended when it delegates a function so the delegate stack can act in a Last-In-First-Out (LIFO) manner so that if a number of applications are suspended due to delegation requests, the proper application is started in the right order. The delegate stack thus keeps track of which application was the last delegator when multiple layered delegation functions are performed. The delegate stack preferably operates in a LIFO manner although different stack schemes could be used as appropriate.



Step 305 then sets the selected ID to the `delegate_request.delegate_application_id` (delegate ID) value. This step selects the application which will be called to perform the delegated function or functions. The identities of the delegated application can be specifically called by the delegator application or a particular function can be  
5 matched up with an application in a look up table. For example, a PIN match operation may be delegated to different applications depending upon which applications are present on the card. Step 307 then sets the `application_command` parameter to the value stored in the `delegate_request.application_command` parameter. This step specifies the command to be delegated to the delegate application. Applications typically have the ability to  
10 process many different commands. Alternatively, the entire application could be executed to perform one or more functions. The delegator application can choose which command it is delegating to another application. Step 309 then sends the `application_command` to the AAM operating system for execution by the delegatee application. The delegator application is then suspended (or interrupted). Any data that  
15 is required to pass between the applications is transferred via the Public memory space.

Figure 4 is a flow chart of the steps for performing a "return delegation control" command by the delegatee application. This command is executed by the operating system when a delegated application has completed its delegated function. Step 401 gets `application_responses` from the Public memory space of the delegated  
20 AAM. The response data is passed in the Public memory segment of the delegatee AAM. Step 403 then sets the `delegate_response.status` variable to a success condition. This

means that a delegation operation has been successfully completed. Step 405 sets the `delegate_response.application_responses` parameter to the `application_responses` values which were stored in the Public segment of the delegatee application.

Step 407 sets the `delegate_response.delegate_application_id` parameter to  
5 `selected_file.application_id` (the delegatee application ID). Step 409 pops the top (i.e.,  
reads the last data stored in the stack) `delegate_application_id` from the  
`delegate_id_stack`. This information indicates the identity of the delegator application for  
the command which was just delegated and completed by the delegated application. Step  
411 sets the `select_file.application_id` value to the `delegator_application_id` value. This  
10 selects the delegator application which was identified from the delegate ID stack as the  
current application which will resume running. The Dynamic data for the delegator  
application will be retrieved for the delegator application from its stored location so that  
the application will continue to execute where it left off with all data intact but will also  
have the response information from the delegated function. In step 413, the  
15 `delegate_response` data is sent to the current application for further processing. The  
response data is passed through the Public data space which could be the same physical  
RAM memory location because all applications share the physical volatile memory space.

Figure 5 shows a flow chart of the steps involved for inquiring about a  
delegator ID when a delegate command is received by a delegated application. The  
20 delegated application may need to know the identity of the delegator because it may  
perform operations differently for different delegator applications. For example, an

airline loyalty program may need to know if awarded frequent flyers will be based on actual dollars processed or a lump sum award for some other activity such as performing a bill payment operation. This information could be passed to the delegated application as a variable or could be ascertained using an inquiry. The delegator inquiry operation  
5 could be implemented as a primitive as previously described.

Step 501 receives the `delegator_id_enq_request` from the AAM operating system. The request is used to identify the identity of the delegator. Step 503 checks if the `delegate_id_stack` is empty. If the stack is empty, then no delegation operations have occurred and no applications have been suspended. Thus step 511 sets the  
10 `delegator_id_enq_response.status` parameter to a failure indicator. Step 513 then sets the value of `delegator_is_enq_request.error_cause` to a value indicating "no delegator application." There is no delegator application. The process then continues with step 509.

If the `delegate_id_stack` is not empty, than one or more delegations have  
15 occurred. In that case, step 505 sets the `delegator_id_enq_response.status` parameter to a value indicating "success". Step 507 then sets the `delegator_id_enq_response.delegator_application_id` parameter to the value stored in `delegate_id_stack.delegator_application_id`. This sets the inquiry response to indicate the delegator application ID at the top of the stack. As explained above, the stored data at the top of the stack indicates  
20 the last delegator application to call a delegate function. Step 509 then sends the

delegator\_id\_enq\_response back to the AAM operator system which delivers the information to the application or IFD entity requesting the information.

Figure 6 shows an example of a block diagram of an integrated circuit located on an IC card chip which can be used in conjunction with the invention. The integrated circuit chip is located on a chip on the card. The IC chip preferably includes a  
5 central processing unit 601, a RAM 603, a EEPROM 605, a ROM 607, a timer 609, control logic 611, I/O ports 613 and security circuitry 615, which are connected together by a conventional data bus 617 or other conventional means.

Control logic 611 in the smart card provides sufficient sequencing and  
10 switching to handle read-write access to the card's memory through the input/output ports 612. CPU 601 in conjunction with control logic 611 can perform many different functions including performing calculations, accessing memory locations, modifying memory contents, and managing input/output ports. Some IC cards also include a coprocessor for handling complex computations like cryptographic algorithms.

15 Input/output ports 613 are used for communication between the card and an IFD which transfers information to and from the card. Timer 609 (which generates and/or provides a clock pulse) drives the control logic 611, CPU 601 and other components requiring a clock signal through the sequence of steps that accomplish functions including memory access, memory reading and/or writing, processing, and data communication. Security  
20 circuitry 615 (which is optional) preferably includes fusible links that connect the input/output lines to internal circuitry as required for testing during manufacture, but

which are destroyed upon completion of testing to prevent later access. The Static memory space is preferably mapped to memory locations in EEPROM 605 which is non-volatile. The Dynamic memory space is preferably mapped to RAM 603 which is volatile memory which has quick access. The Public memory space is also preferably mapped to RAM 603 which is volatile memory. The Dynamic data and Public data will be stored in different portions of RAM 603, while RAM is identified as a preferred non-volatile memory and EEPROM is identified as a preferred volatile memory. Other types of memory could also be used with the same characteristics.

Figures 7A, 7B and 7C illustrate an example of a delegation function being performed in order to process multiple applications on an IC card. Figure 7A shows a first application being executed as denoted with a double ringed circle 701. At some point during the execution of the first application, a delegation function 702 is called to delegate an operation to the second application which is indicated by circle 703. Also shown in Figure 7A is an empty delegator ID stack 705. Since the stack is empty, there is no data associated with it and it is shown only for illustrative purposes.

The multiple application operating system receives the delegate command and interrupts the execution of the first application 701 and gives control of the integrated circuit to application 703 as shown in Figure 7B. The execution of the second application 703 is illustrated with a double ringed circle. The term "gives control" means that the microprocessor and other circuitry on the card will process the instructions and allocate memory space for the application which is delegated. When the delegate command is

processed, the delegator ID 707 is placed on top of the stack 705. The delegator ID stack is operated in a LIFO manner. Also shown in Figure 7B is a third application 709 resident on the card. At some point during the execution of the second application, a delegate function 711 is called to delegate the operation to the third application.

5           The multiple application operating system receives the delegate command 711 shown in Figure 7B interrupts the execution of the second application 703 and gives control of the integrated circuit to the third application 709 as shown in Figure 7C. When the delegate command is processed, the delegator ID 713 of the second application is pushed onto the delegator ID stack 705. The delegator ID 707 of the first application  
10   whose execution is still interrupted is pushed down in the stack consistent with a LIFO stack management. Thus when the third application has finished its execution, the delegator ID at the top of the stack is popped to indicate that execution of the second application should be resumed first. The delegator ID 707 from the first application will then be at the top of the stack so that when the second application is finished executing,  
15   the first application will resume its execution.

Additional applications can be managed by the delegator ID stack in a similar manner. By interrupting the execution of the applications when a delegate command is processed and keeping track of the order of delegations, the security and integrity of the data for each individual application can be maintained which is important  
20   because IC cards will store data for applications which is private to the card user such as account numbers, social security number, address and other personal information.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise numerous apparatus, systems and methods which, although not explicitly shown or described herein, embody the principles of the invention and are thus within the spirit and scope of the invention.

5           The scope of the present disclosure includes any novel feature or combination of features disclosed therein either explicitly or implicitly or any generalisation thereof irrespective of whether or not it relates to the claimed invention or mitigates any or all of the problems addressed by the present invention. The application hereby gives notice that new claims may be formulated to such features during the  
10 prosecution of this application or of any such further application derived therefrom. In particular with reference to the appended claims, features from dependant claims may be combined with those of the independent claims in any appropriate manner and not merely in the specific combinations enumerated in the claims.

WE CLAIM:

- 2 1. An integrated circuit card comprising:  
3 a microprocessor; a volatile memory coupled to said  
4 microprocessor; a non-volatile memory coupled to said microprocessor; and a plurality of  
5 applications stored in said non-volatile memory, wherein upon execution of each said  
6 application, said microprocessor allocates for each said executing application an  
7 associated data memory space comprising at least a volatile memory segment for  
8 referencing temporary data and a non-volatile memory segment for referencing static  
9 data; and further comprising means for delegating the performance of a function from a  
10 first executing application to a second executing application.
- 1 2. The integrated circuit card of claim 1, wherein said non-volatile memory segment  
2 is divided into at least two regions, including a public region and a dynamic region.
- 1 3. The integrated circuit card of claim 2, wherein said public region is used to share  
2 data between said first and second applications.
- 1 4. The integrated circuit card of claim 2 or claim 3, wherein said dynamic region is  
2 used to reference temporary data utilized during an application's execution.



1 5. The integrated circuit card of any preceding claim, further comprising at least one  
2 register coupled to said microprocessor which is used to determine the starting locations  
3 of each of said segments.

1 6. The integrated circuit card of any preceding claim, further comprising at least one  
2 register coupled to said microprocessor which is used to determine the top locations of  
3 each of said segments.

1 7. The integrated circuit card of any preceding claim, further comprising at least one  
2 register coupled to said microprocessor which is used as a local dynamic pointer.

1 8. The integrated circuit card system of any preceding claim, wherein each said  
2 application comprise a plurality of program instructions and wherein at least one of said  
3 program instructions when executed causes said memory referenced by said volatile  
4 memory segment to be accessed.

1 9. The integrated circuit card of any preceding claim, wherein said volatile memory  
2 segment references RAM and said non-volatile memory segment references EEPROM.

1 10. A method for processing a plurality of applications stored in a memory of an  
2 integrated circuit:

1                   selecting a first application for execution;  
2                   allocating a data space for said first application including at least  
3 two memory segments comprising a volatile memory segment for referencing temporary  
4 data and a non-volatile memory segment for referencing static data;  
5                   executing said first application, interrupting execution of said first  
6 application and saving data referenced by said volatile memory segment;  
7                   executing a second application;  
8                   utilizing said saved data from said volatile memory segment for  
9 execution of said first application; and  
10                  completing said execution of said first application.

1 11. The method of claim 10, wherein said first application's identity is stored in a data  
2 stack during said delegation step.

1 12. The method of claim 11, wherein said data stack is accessed following said  
2 completion of said second application.

1 13. The method of claim 11 or 12, further including the step of inquiring said first  
2 application's identity by accessing said delegator stack.

1 14. The method of any of claims 10 to 13, wherein said non-volatile memory segment  
2 is divided into at least two regions, including a public region and a dynamic region.

1 15. The method of claim 14, wherein said public region is used to share data between  
2 said first application and said second application.

1 16. The method of claim 14 or 15, wherein data referenced by said dynamic region is  
2 utilized during the execution of said first application.

1 17. The method of any of claims 10 to 15, further including the step of allocating a  
2 second data space including at least two memory segments for said second application.

1 18. The method of claim 17, wherein said second data space's segments comprise a  
2 volatile memory segment for referencing temporary data and a non-volatile memory  
3 segment for referencing static data.

1 19. The method of claim 18, wherein said second application's non-volatile segment  
2 is divided into at least two regions, including a public region and a dynamic region.

1 20. The method of claim 19, wherein said second application's public region is used  
2 to share data between said first and second applications.

1 21. The method of claim 19 or 20, wherein said data referenced by second  
2 application's dynamic region is utilized during said execution of said second application.

1 22. The method of any of claims 10 to 21, further including the step of delegating use  
2 of said microprocessor from said second application to a third application stored on said  
3 IC card.

1 23. The method of claim 22, wherein a third data space for said third application is  
2 allocated which includes a volatile memory segment for referencing temporary data and  
3 non-volatile memory segment for referencing static data, wherein said third application's  
4 volatile segment includes a public and dynamic portion.

1 24. An apparatus for processing a plurality of applications stored in a memory of a  
2 single integrated circuit card comprising:  
3 means for allocating a data space comprising at least a non-volatile  
4 memory segment for referencing static data and a volatile memory segment for  
5 referencing temporary data; means for executing a first application; means for  
6 interrupting execution of said first application, means for saving data from at least a  
7 portion of said volatile memory segment; and means for executing a second application;  
8 means for retrieving said saved data; and means for completing said execution of said  
9 first application.

1 25. The apparatus of claim 24, further including means for storing said first  
2 application's identity on a data stack.

1 26. The apparatus of claim 25, further including means for inquiring of said first  
2 application's identity.

1 27. The apparatus of any of claims 24 to 26, wherein said first application's non-  
2 volatile memory segment is divided into at least two regions, including a public region  
3 and a dynamic region.

1 28. The apparatus of claim 27, wherein said public region references random access  
2 memory.

1 29. The apparatus of claim 27 or 28, wherein said dynamic region references random  
2 access memory.

1 30. The apparatus of any of claims 24 to 29, further including means for allocating a  
2 second data space including at least two segments for said second application.

1 31. The apparatus of claim 30, wherein said second data space includes a volatile  
2 memory segment for referencing temporary data and a non-volatile memory segment for  
3 referencing static data.

1 32. The apparatus of claim 31, wherein said second data space's non-volatile segment  
2 is divided into at least two regions, including a public region and a dynamic region.

1 33. The apparatus of claim 32, wherein said public region references random access  
2 memory.

1 34. The apparatus of claim 32 or 33, wherein said dynamic region references random  
2 access memory.

1 35. The apparatus of any of claims 24 to 34, further including means for delegating  
2 operation of said IC card from said second application to a third application stored on  
3 said IC card.

1 36. The apparatus of claim 35, wherein a third data space for said third application is  
2 allocated which includes a volatile memory segment for referencing temporary data and  
3 non-volatile memory segment for referencing temporary data, wherein said third  
4 application's volatile memory segment includes a public and dynamic portion.

1 37. A system for processing a plurality of applications stored on an IC card  
2 comprising:  
3 a non-volatile memory coupled to a databus;

4                   a volatile memory coupled to said databus;  
5                   a first and second application program stored in said non-volatile memory,  
6   wherein each application has an associated identifier;  
7                   a data stack accessible by said databus for storing said applications'  
8   identifier if said application is interrupted during its execution;  
9                   processor means for executing instructions from said application programs  
10   wherein said processor means allocates a data memory space for said application which is  
11   being executed and said data memory space is mapped to at least one address in said non-  
12   volatile memory and at least one address in said volatile memory; and  
13                   wherein said processor means interrupts said first application at least once  
14   during its execution to execute said second application.

1   38.    The system of claim 37, wherein data memory space comprises at least a volatile  
2   memory segment for referencing temporary data stored in said volatile memory and a  
3   non-volatile memory segment for referencing static data stored in said non-volatile  
4   memory.

1   39.    The system of claim 37 or 38, further including means for storing said first  
2   application's identity on a data stack.

1   40.    The system of any of claims 37 to 39, further including means for inquiring of  
2   said first application's identity.

1 41. The system of any of claims 38 to 40, wherein said first application's non-volatile  
2 memory segment is divided into at least two regions, including a public region and a  
3 dynamic region.

1 42. The system of claim 41, wherein said public region references random access  
2 memory.

1 43. The system of claim 41 or 42, wherein said dynamic region references random  
2 access memory.

1 44. The system of any of claims 37 to 43, further including means for allocating a  
2 second data space including at least two segments for said second application.

1 45. The system of claim 44, wherein said second data space comprises at least a  
2 volatile memory segment for referencing temporary data and a non-volatile memory  
3 segment for referencing static data.

1 46. The system of claim 45, wherein said second data space's non-volatile segment is  
2 divided into at least two regions, including a public region and a dynamic region.



1 47. The system of claim 46, wherein said public region references random access  
2 memory.

1 48. The system of claim 46, wherein said dynamic region references random access  
2 memory.

1 49. The system of any of claims 37 to 48, further including means for delegating use  
2 of said processor means from said second application to a third application stored on said  
3 IC card.

1 50. The system of claim 49, wherein a third data space for said third application is  
2 allocated which includes a volatile memory segment for referencing temporary data and  
3 non-volatile memory segment for referencing temporary data, wherein said third  
4 application's volatile memory segment includes a public and dynamic portion.

1 51. An integrated circuit card comprising:  
2 a plurality of applications and a microprocessor for controlling  
3 execution of said applications wherein execution of at least one first application is  
4 interrupted and execution is transferred to another second application, further comprising  
5 means for sharing data by said first and second applications and means for resuming  
6 execution of said first application at the appropriate location at least after completion of  
7 execution of said second application.

1 52. The integrated circuit card of claim 51, further comprising means for allocating a  
2 data memory space comprises at least a volatile memory segment for referencing  
3 temporary data stored in said volatile memory and a non-volatile memory segment for  
4 referencing static data stored in said non-volatile memory.

1 53. The integrated circuit card of claim 51 or 52, further including means for storing  
2 said first application's identity on a data stack.

1 54. The integrated circuit card of any of claims 51 to 53, further including means for  
2 inquiring of said first application's identity.

1 55. The integrated circuit card of claim 52, wherein said first application's non-  
2 volatile memory segment is divided into at least two regions, including a public region  
3 and a dynamic region.

1 56. The integrated circuit card of claim 55, wherein said public region references  
2 random access memory.

1 57. The integrated circuit card of claim 55 or 56, wherein said dynamic region  
2 references random access memory.

1 58. The integrated circuit card of any of claims 52 to 57, further including means for  
2 allocating a second data space including at least two segments for said second  
3 application.

1 59. The integrated circuit card of claim 58, wherein said second data space comprises  
2 at least a volatile memory segment for referencing temporary data and a non-volatile  
3 memory segment for referencing static data.

1 60. The integrated circuit card of claim 59, wherein said second data space's non-  
2 volatile segment is divided into at least two regions, including a public region and a  
3 dynamic region.

1 61. The integrated circuit card of claim 60, wherein said public region references  
2 random access memory.

1 62. The integrated circuit card of claim 60 or 61, wherein said dynamic region  
2 references random access memory.

1 63. The integrated circuit card of any of claims 51 to 62, further including means for  
2 delegating use of said processor means from said second application to a third application  
3 stored on said IC card.

- 1 64. An integrated circuit card comprising:
- 2 a microprocessor; a volatile memory coupled to said
- 3 microprocessor; a non-volatile memory coupled to said microprocessor for storing a
- 4 plurality of applications, and adapted for each application to be executed to allocate an
- 5 associated data memory space comprising at least a volatile memory segment for
- 6 referencing temporary data and a non-volatile memory segment for referencing static data
- 7 prior to execution of each said application and further comprising means for delegating
- 8 the performance of a function from a first executing application to a second executing
- 9 application.

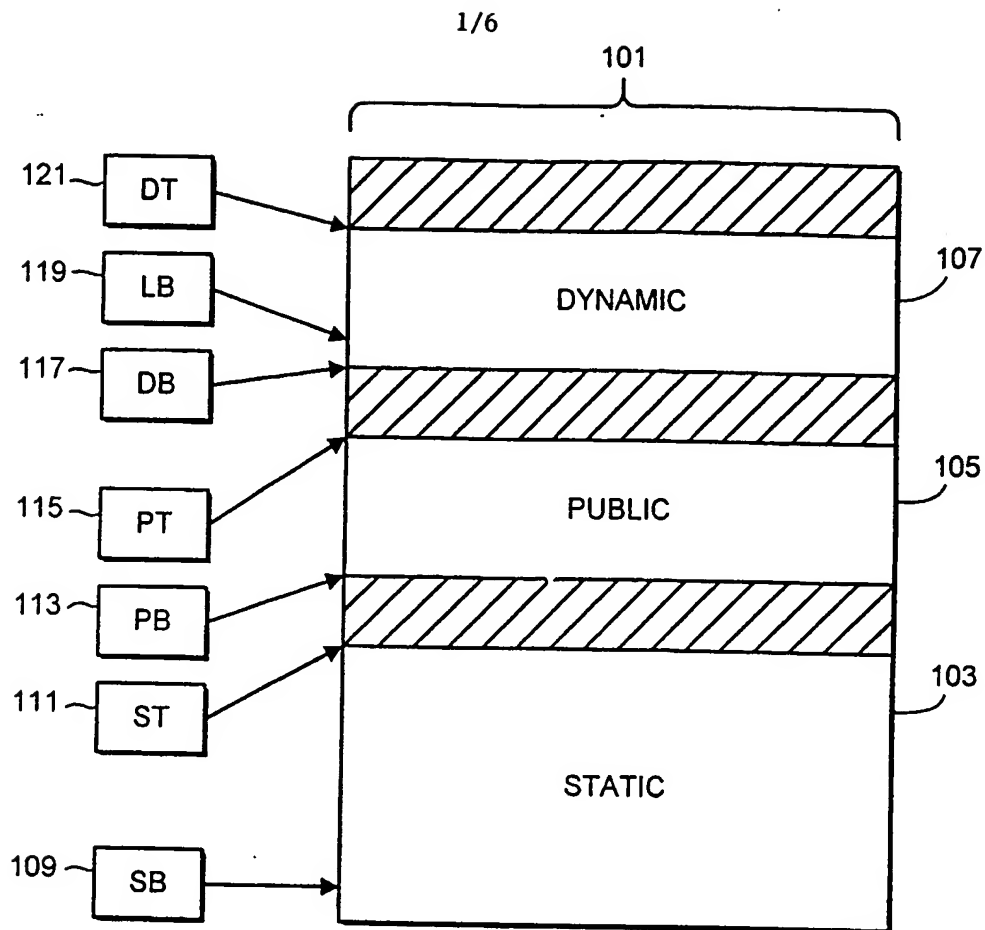


FIG. 1

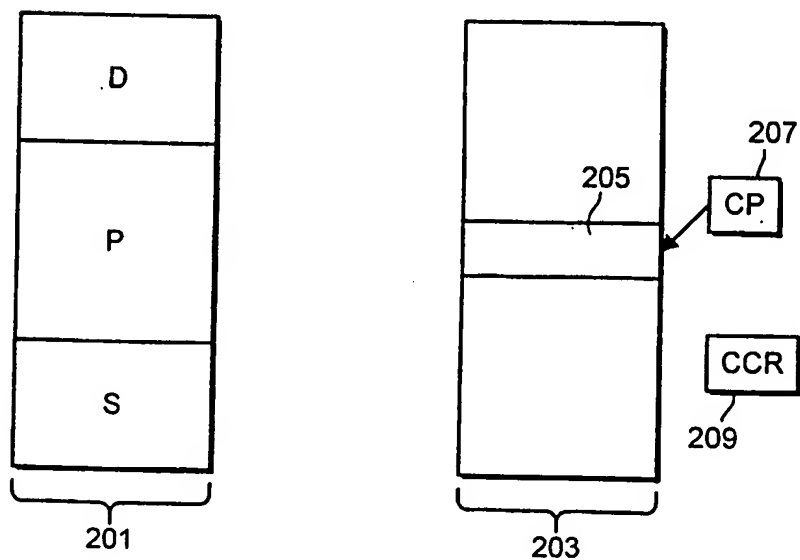
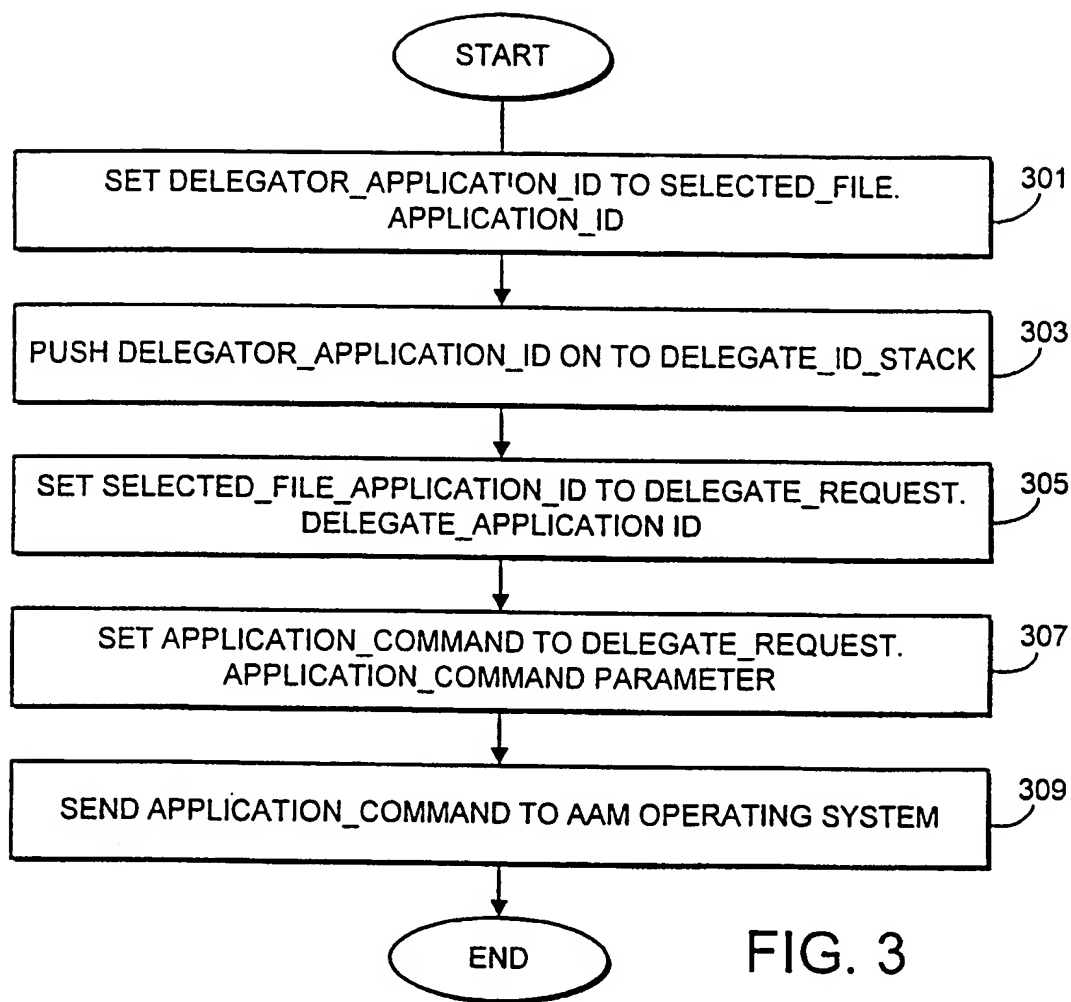
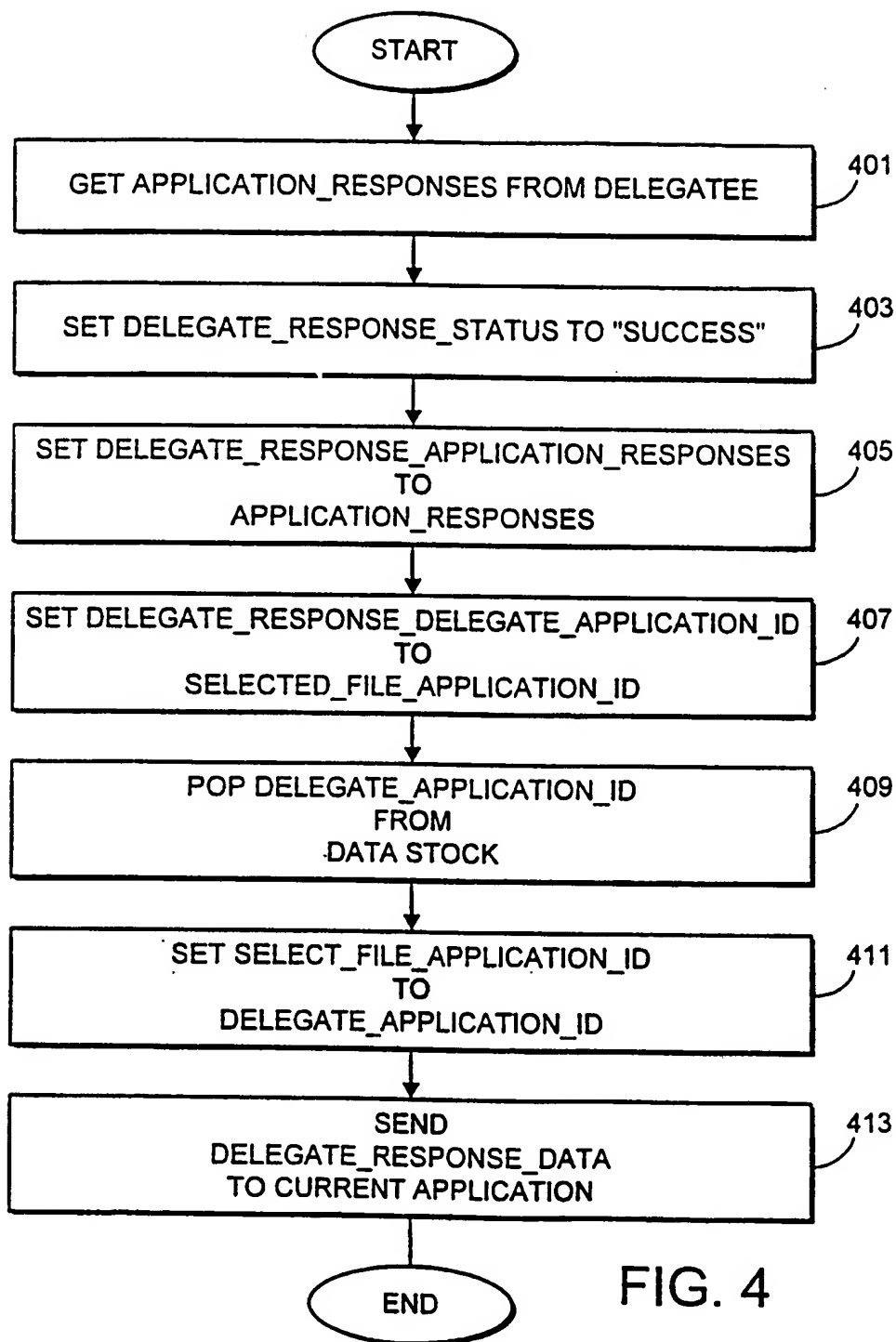


FIG. 2



3/6



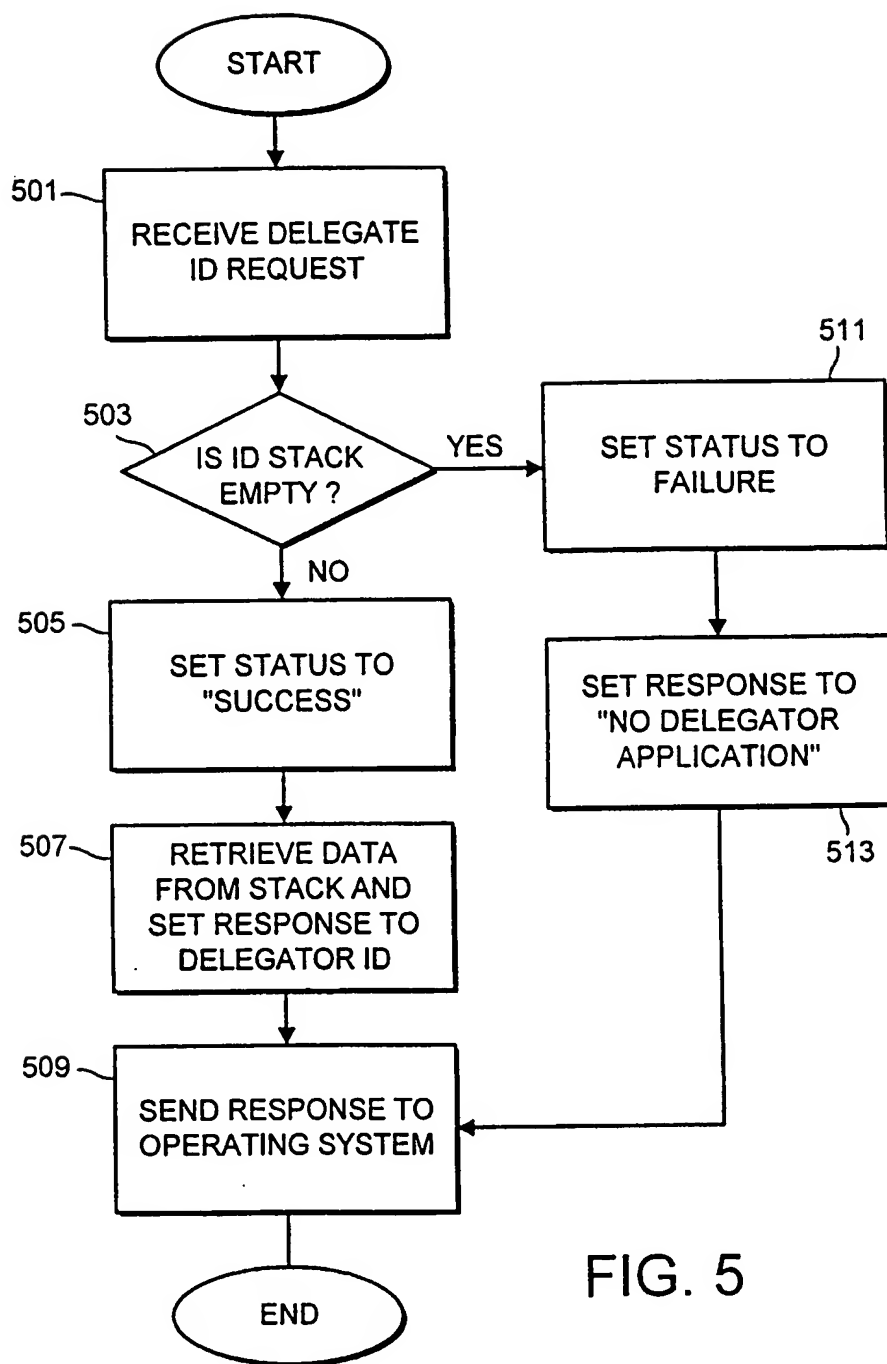


FIG. 5



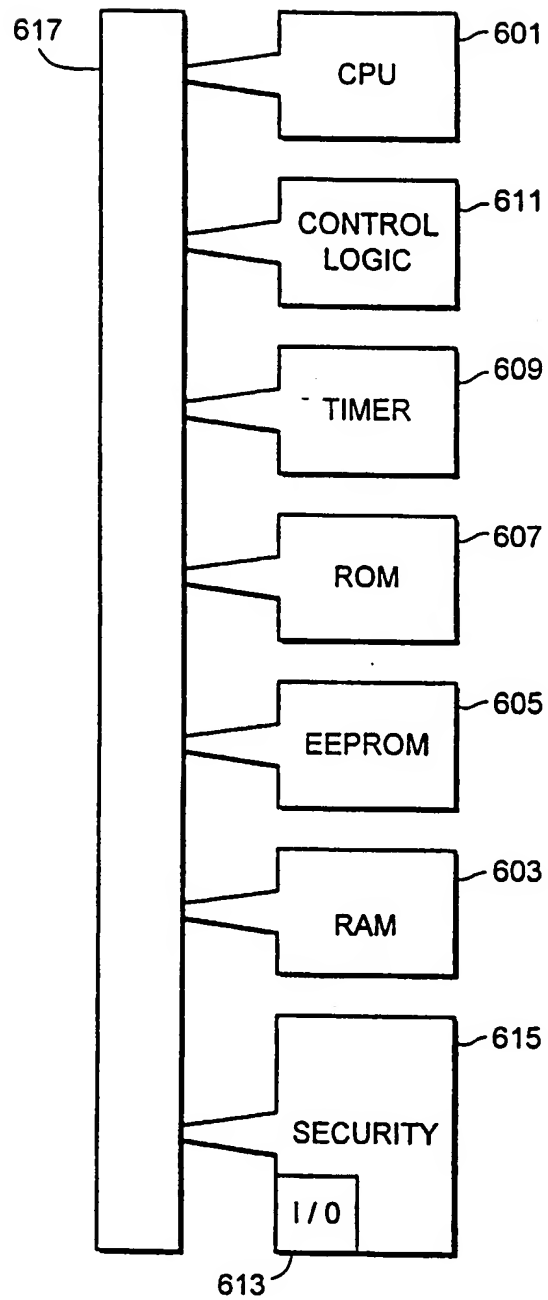


FIG. 6

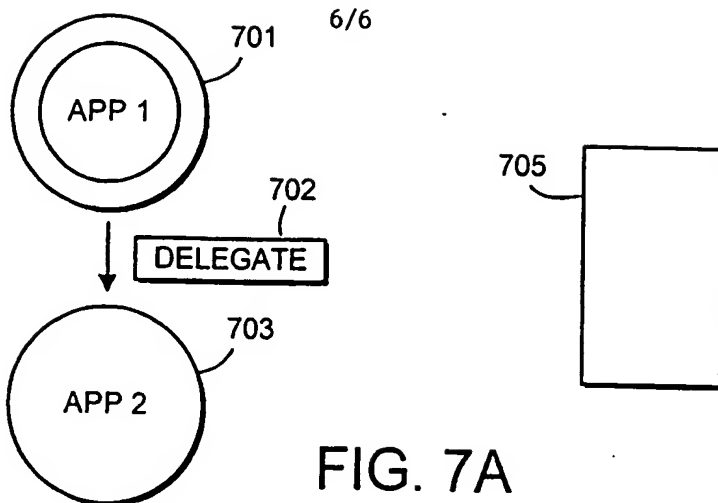


FIG. 7A

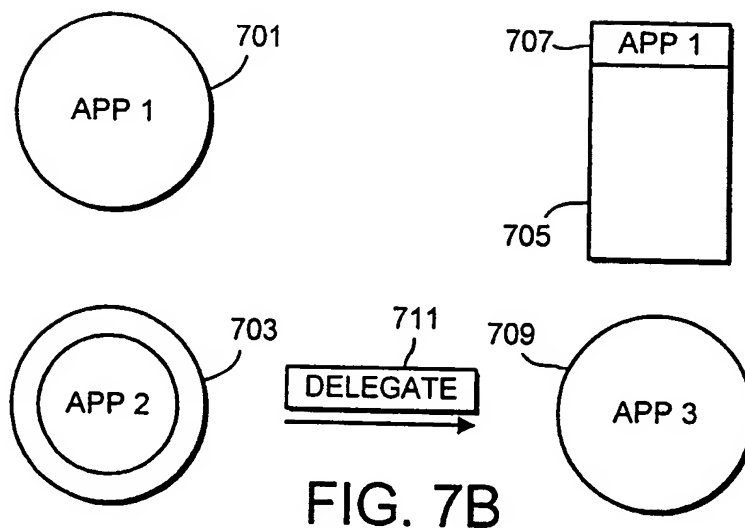


FIG. 7B

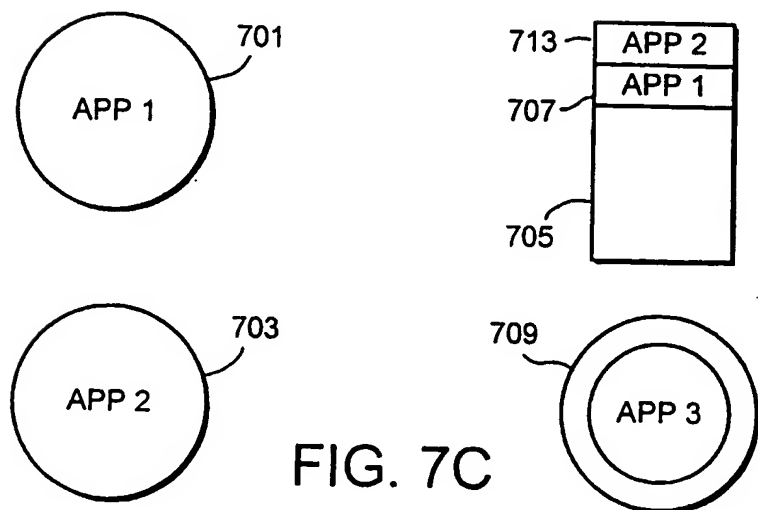


FIG. 7C



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT) -

<p>(51) International Patent Classification <sup>6</sup> : <b>G07F 7/10</b></p>	<b>A3</b>	<p>(11) International Publication Number: <b>WO 98/52159</b></p> <p>(43) International Publication Date: 19 November 1998 (19.11.98)</p>									
<p>(21) International Application Number: <b>PCT/GB98/01390</b></p> <p>(22) International Filing Date: <b>14 May 1998 (14.05.98)</b></p> <p>(30) Priority Data:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">60/046,514</td> <td style="width: 33%;">15 May 1997 (15.05.97)</td> <td style="width: 33%;">US</td> </tr> <tr> <td>60/046,543</td> <td>15 May 1997 (15.05.97)</td> <td>US</td> </tr> <tr> <td>09/064,915</td> <td>23 April 1998 (23.04.98)</td> <td>US</td> </tr> </table> <p>(71) Applicant: <b>MONDEX INTERNATIONAL LIMITED</b> [GB/GB]; 47-53 Cannon Street, London EC4M 5SQ (GB).</p> <p>(72) Inventors: <b>EVERETT, David</b>, Barrington; 31 Ashdown Avenue, Saldean, Brighton, East Sussex BN2 8AH (GB). <b>MILLER, Stuart, James</b>; 9 Woodford Green, The Warren, Bracknell, Berks RG12 9YQ (GB). <b>PEACHAM, Anthony, David</b>; 4 Lynwood, Groombridge, Tunbridge Wells, Kent TN3 9LX (GB). <b>SIMMONS, Ian, Stephens</b>; The Elms, School Road, Broughton, Cambs PE17 3AT (GB). <b>RICHARDS, Timothy, Philip</b>; 32 Craig Mount, Radlett, Herts WD7 7LW (GB). <b>VINER, John, Charles</b>; Hydes, Woodlands Lane, Windlesham (GB).</p> <p>(74) Agent: <b>POTTER, Julian, Mark</b>; D. Young &amp; Co., 21 New Fetter Lane, London EC4A 1DA (GB).</p>		60/046,514	15 May 1997 (15.05.97)	US	60/046,543	15 May 1997 (15.05.97)	US	09/064,915	23 April 1998 (23.04.98)	US	<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p> <p>(88) Date of publication of the international search report: <b>1 July 1999 (01.07.99)</b></p>
60/046,514	15 May 1997 (15.05.97)	US									
60/046,543	15 May 1997 (15.05.97)	US									
09/064,915	23 April 1998 (23.04.98)	US									
<p>(54) Title: <b>MULTI-APPLICATION IC CARD WITH DELEGATION FEATURE</b></p>											
<p>(57) Abstract</p> <p>A multi-application IC card which processes two or more applications using an Application Abstract Machine architecture. The AAM architecture only allows one application to be executed at a time and allows for shared processing by performing a delegation function to a second application. A data space for each application is allocated when the application is selected to be executed. The data space includes a volatile and non-volatile region. The delegation, function temporarily interrupts the execution of the first application, saves the temporary data of the first application, shares any data needed with the second application and the second application is executed until the delegated task is completed. The first application then retrieves the saved data and completes its execution. A delegator stack is used to keep track of the delegator's identity when multiple delegations occur. The AAM model allows for a high level of security while transferring data between applications.</p>											

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LJ	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 98/01390

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 666 550 A (E.K. DE JONG ) 9 August 1995 see abstract; claims; figures ---	1,10,24, 37,51,64
A	EP 0 647 902 A (IBM) 12 April 1995 see abstract; claims; figures ---	1-64
A	EP 0 751 460 A (SUN MICROSYSTEMS) 2 January 1997 -----	



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

### \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "Z" document member of the same patent family

Date of the actual completion of the international search

7 May 1999

Date of mailing of the international search report

10. 05. 1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

David, J

# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/GB 98/01390

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0666550 A	09-08-1995	AT 152539 T AU 681754 B AU 1546095 A CA 2182783 A CN 1150850 A DE 69402955 D DE 69402955 T FI 963111 A JP 9508733 T WO 9522126 A NZ 278967 A US 5802519 A	15-05-1997 04-09-1997 29-08-1995 17-08-1995 28-05-1997 05-06-1997 14-08-1997 07-08-1996 02-09-1997 17-08-1995 24-04-1997 01-09-1998
EP 0647902 A	12-04-1995	JP 7121373 A US 5737605 A	12-05-1995 07-04-1998
EP 0751460 A	02-01-1997	US 5799314 A JP 9034732 A	25-08-1998 07-02-1997

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**